Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 1 of 31

1. JASON S. LEIDERMAN, SBN 203336 jay@criminal-lawyer.me
2. ERIC J. LINDGREN, SBN 288542

eric@criminal-lawyer.me

1. LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300
2. Ventura, California 93003

Tel: 805-654-0200

5 Fax: 805-654-0280

1. TOR EKELAND, PRO HAC VICE tor@torelekand.com
2. TOR EKELAND, P.C.

155 Water Street

1. Brooklyn, NY 11201 Tel: 718-285-9279

9 Fax: 718-504-5417

10 Attorneys for Defendant MATTHEW KEYS

11

1. UNITED STATES DISTRICT COURT
2. EASTERN DISTRICT OF CALIFORNIA 14

15

1. UNITED STATES,
2. Plaintiff,
3. v.
4. MATTHEW KEYS,
5. Defendant.

21

) Case No.: 13-CR-00082 KJM

)

# ) NOTICE OF MOTION AND MOTION TO

) **SUPPRESS EVIDENCE; MEMORANDUM**

) **OF POINTS AND AUTHORITIES**

)

)

|  |  |
| --- | --- |
| Date: | January 29, 2014 |
| Time: | 9:00 am |
| Place: | Courtroom 3 |

)

)

)

)

)

)

)

)

22 )

# TO THE COURT AND THE UNITED STATES, THROUGH THE UNITED STATES

1. **ATTORNEY:**
2. **PLEASE TAKE NOTICE THAT** on the above date and time, or as soon thereafter as the
3. matter can be heard in the above designated courtroom, or such other courtroom to which said motion is
4. assigned, Defendant Matthew Keys (“Defendant” or “Mr. Keys”), by and through counsel, will move

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 2 of 31

1. the court to issue an order suppressing evidence seized as a result of a search and seizure by police
2. officers, to wit:
3. 1. The audio recording and any transcript of Mr. Keys’ statement to investigators on October 4, 4 2012.
4. 2. The perceptions, recollections and observations of the officers related to that taped statement.
5. 3. Mr. Keys’ written statement to the government dated October 4, 2012.
6. 4. All property and information seized during the October 4, 2012 execution of a search warrant
7. on Mr. Keys’ New Jersey residence.
8. 5. Any other evidence the court finds unlawfully obtained and the fruits thereof.
9. This motion is made under Rule 12(b)(3)(C) of the Federal Rules of Criminal Procedure on the
10. ground that the search and seizure violated Defendant’s rights under the Fourth and Fifth Amendments
11. to the United States Constitution.
12. This motion is based on the attached points and authorities, the testimony of any witnesses at the
13. hearing, the attached declarations of Defendant’s counsel, the files and records in this action, and any
14. further evidence or argument that the Court may properly receive at or before the hearing 16

17 Dated: December 13, 2013

18

By:\_ */s/ Jay Leiderman*

1. Jason S. Leiderman
2. Eric J. Lindgren

LAW OFFICES OF JAY LEIDERMAN

21

1. By:\_ */s/ Tor Ekeland*
2. Tor Ekeland

TOR EKELAND, P.C.

24

25 Attorneys for Defendant

MATTHEW KEYS

26

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 3 of 31

# TABLE OF CONTENTS

# [TABLE OF AUTHORITIES v](#_bookmark0)

# [MEMORANDUM OF POINTS AND AUTHORITIES 1](#_bookmark1)

# [INTRODUCTION 1](#_bookmark2)

# [STATEMENT OF FACTS 1](#_bookmark3)

# [I. THE SEARCH WARRANT AND AFFIDAVIT 2](#_bookmark4)

1. [A. EARLY DECEMBER 2010 “SUSPICIOUS” E-MAILS 3](#_bookmark5)
2. [B. COMMUNICATION BETWEEN MERCER AND MR. KEYS REGARDING](#_bookmark6)
3. [ANONYMOUS. 4](#_bookmark6)
4. [C. INTERNAL INVESTIGATION OF THE DECEMBER 14, 2010 EDITS TO THE LOS](#_bookmark7)
5. [ANGELES TIMES WEBSITE. 5](#_bookmark7)
6. [D. MR. KEYS PUBLISHED ARTICLES ACKNOWLEDGING ACCESS TO “TOP LEVEL](#_bookmark8)
7. [HACKERS” USING THE NAME “AESCracked.” 5](#_bookmark8)
8. [E. CHAT LOGS SEIZED DURING OTHER INVESTIGATIONS 5](#_bookmark9)
9. [F. OTHER IP ADDRESS INFORMATION. 6](#_bookmark10)
10. [G. JUSTIFICATION FOR THE BREADTH OF THE SEARCH. 6](#_bookmark11)

# [II. EXECUTION OF THE WARRANT. 10](#_bookmark12)

# [ARGUMENT 10](#_bookmark13)

# [I. THE SEARCH WARRANT AUTHORIZED AN OVERBROAD GENERAL SEARCH OF](#_bookmark14)

# [ALL OF MR. KEYS’ ELECTRONIC MEDIA 10](#_bookmark14)

1. [A. IN ORDER TO CONDUCT WHOLESALE SEIZURES OF ELECTRONIC MEDIA, THE](#_bookmark15)
2. [GOVERNMENT MUST PRESENT A FACTUAL BASIS FOR DOING SO, IT MUST FOLLOW](#_bookmark15)
3. [A SEGREGATION PROTOCOL FOR IDENTIFYING RELEVANT INFORMATION, AND IT](#_bookmark15) 24 [MUST RETURN IRRELEVANT INFORMATION. 12](#_bookmark15)

25 [B. THE WARRANT COMPLETELY IGNORES CHIEF JUDGE KOZINSKI’S GUIDELINES](#_bookmark16) 26 [IN *COMPREHENSIVE DRUG TESTING III* 14](#_bookmark16)

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 4 of 31

# [II. AT THE TIME ANDREWS APPLIED FOR THE WARRANT, THE FACTS](#_bookmark17)

# [SUPPORTING PROBABLE CAUSE TO BELIEVE MR. KEYS POSSESSED ANY EVIDENCE](#_bookmark17)

# [WERE STALE 16](#_bookmark17)

# [III. THE AFFIDAVIT CONTAINS DELIBERATE OR RECKLESS](#_bookmark18)

# [MISREPRESENTATIONS AND OMISSIONS REQUIRING A *FRANKS* HEARING 18](#_bookmark18)

1. [A. ANDREWS’ AFFIDAVIT CONTAINS DELIBERATE OR RECKLESSLY-MADE](#_bookmark19)
2. [STATEMENTS AND OMISSIONS 19](#_bookmark19)
3. [B. WITH THE FALSE STATEMENTS AND OMISSIONS CORRECTED, THE AFFIDAVIT](#_bookmark20)
4. [DOES NOT SUPPORT A FINDING OF PROBABLE CAUSE. 20](#_bookmark20)

# [IV. THE FRUIT OF THE POISONOUS TREE DOCTRINE REQUIRES SUPPRESSION OF](#_bookmark21)

# [WRITTEN AND RECORDED STATEMENTS OF MR. KEYS. 21](#_bookmark21)

# [V. MR. KEYS’ *MIRANDA* WAIVER WAS INVALID BECAUSE IT WAS NOT](#_bookmark22)

# [VOLUNTARY, KNOWING AND INTELLIGENT. 22](#_bookmark22)

1. [A. MR. KEYS INVOLUNTARILY WAIVED HIS *MIRANDA* RIGHTS. 22](#_bookmark23)
2. [B. MR. KEYS DID NOT KNOWINGLY AND INTELLIGENTLY WAIVE HIS *MIRANDA*](#_bookmark24)
3. [RIGHTS. 23](#_bookmark24)

# [CONCLUSION 25](#_bookmark25)

18

19

20

21

22

23

24

25

26

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 5 of 31

1

# 2 Federal Cases

**TABLE OF AUTHORITIES**

3 *Brown v. Illinois*, 422 U.S. 590 (1975) 21

1. *Chism v. Washington State*, 661 F.3d 380 (9th Cir. 2011) 20
2. *Colorado v. Connelly*, 479 U.S. 157 (1986) 22

6 *Colorado v. Spring*, 479 U.S. 564 (1987) 22, 24

7 *Coolidge v. New Hampshire*, 402 U.S. 443 (1971) 10

8 *Derrick v. Peterson*, 924 F.2d 813 (9th Cir. 1990) 22, 23

9 *Durham v. United States*, 403 F.2d 190 (9th Cir. 1968) 16

10 *Franks v. Delaware*, 438 U.S. 154 (1978) (“*Franks*”) 18, 20, 21

11 *Gladden v. Unsworth*, 396 F.2d 373 (9th Cir. 1968) 22, 23

12 *In re Grand Jury Subpoenas Dated December 10, 1987*, 926 F.2d 847 (9th Cir. 1991) 11

13 *Jackson v. Denno*, 378 U.S. 368 (1964) 22

14 *Lucero v. Kerby*, 133 F.3d 1299 (10th Cir. 1998) 23

15 *Miranda v. Arizona*, 384 U.S. 436 (1966) 22, 23, 24

16 *Moran v. Burbine*, 475 U.S. 412 (1986) 23

17 *Nardone v. United States*, 308 U.S. 338 (1939) 21

18 *Nix v. Williams*, 467 U.S. 431 (1984) 21

19 *Payton v. New York*, 445 U.S. 573 (1980) 10

20 *Sample v. Eyman*, 469 F.2d 819 (9th Cir. 1972) 24

21 *Sgro v. United States*, 287 U.S. 206 (1932) 16

22 *Tague v. Louisiana*, 444 U.S. 469 (1980) 23

23 *Taylor v. Maddox*, 366 F.3d 992 (9th Cir. 2004) 23

1. *United States v. Chesher*, 678 F.2d 1353 (9th Cir. 1982) 19
2. *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009) (“*CDT II*”) 14
3. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) (“*CDT III*”) 11, 13,

27 14, 15

28 *United States v. DeLeon*, 979 F.2d 761 (9th Cir. 1992) 19

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 6 of 31

1. *United States v. Dozier*, 844 F.2d 701 (9th Cir. 1988) 16
2. *United States v. Frank*, 956 F.2d 872 (9th Cir. 1991) 24
3. *United States v. Gann*, 732 F.2d 714 (9th Cir. 1984) 16
4. *United States v. Grant*, 682 F.3d 827 (9th Cir. 2012) 16
5. *United States v. Greany*, 929 F.2d 523 (9th Cir. 1991) 16
6. *United States v. Greathouse*, 297 F.Supp.2d 1264 (D. Or. 2003) 17, 18
7. *United States v. Guerrero*, 847 F.2d 1363 (9th Cir. 1988) 22
8. *United States v. Hill*, 459 F.3d 966 (9th Cir. 2006) 13, 14
9. *United States v. Jawara*, 474 F.3d 565 (9th Cir. 2007) 19
10. *United States v. Lacy*, 119 F.3d 742 (9th Cir. 1997) 16, 17
11. *United States v. Montoya-Arrubla*, 749 F.2d 700 (11th Cir. 1985) 24
12. *United States v. Smith*, 638 F.2d 131 (9th Cir. 1981) 22
13. *United States v. Stanert*, 762 F.2d 775 (9th Cir. 1985) 19

14 *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982) 12, 13, 14

1. *United States v. Towne*, 997 F.2d 537 (9th Cir. 1993) 11
2. *Wong Sun v. United States*, 371 U.S. 471 (1963) 21

# Statutes

18 18 U.S.C. § 1030 1

19 18 U.S.C. § 3501 23

20 18 U.S.C. § 371 1

# 21 Constitutional Provisions

22 U.S. Const. amend. IV 1, 11, 13, 14

23 U.S. Const. amend. V 1

24

25

26

27

28

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 7 of 31

# MEMORANDUM OF POINTS AND AUTHORITIES

1. **INTRODUCTION**
2. This case involves a seizure that goes to the very heart of what the Fourth Amendment prohibits.
3. For no reason other than allowing the FBI to fish for electronic data, a magistrate authorized and the
4. government executed a wholesale seizure of Defendant Matthew Keys’ electronic media. The warrant
5. was unsupported by any facts requiring such a seizure and unaccompanied by any protocol designed to
6. prevent a general rummaging, and therefore the seizure violated the Fourth Amendment’s prohibition on
7. general warrants.
8. This general search led directly to a police interview of Mr. Keys, during which he involuntarily
9. waived his Fifth Amendment right against self-incrimination. Additionally, the circumstances
10. surrounding the interview show that Mr. Keys did not participate knowingly, voluntarily, or
11. intelligently. As such, Mr. Keys’ statements must be suppressed as violative of his Fifth Amendment
12. rights and of the fruit of the poisonous tree doctrine.

# STATEMENT OF FACTS

1. Mr. Keys was indicted in a three-count indictment in March 14, 2013. (Docket entry # 1.)
2. Count 1 alleges a conspiracy to intentionally cause unauthorized damage to a protected computer via a
3. knowing transmission of a program, information, code, and command, in violation of 18 U.S.C. §§ 371
4. and 18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B). Count 2 alleges a substantive violation of 18 U.S.C.
5. §§ 1030(a)(5)(A), (c)(4)(B). And count 3 alleges a knowing attempted transmission of a program,
6. information, code, and command with the intent to cause damage to a protected computer in violation of 21 18 U.S.C. §§ 1030(a)(5)(A), (b).

22 These charges stem from edits to one paragraph of a story on the Los Angeles Times website on

23 December 14, 2010. That day, using the Los Angeles Times/Tribune Company’s content management

1. system (“CMS”), the user “ngarcia” allegedly altered a paragraph of a latimes.com story. The article’s
2. title and byline originally appeared as follows:
3. Pressure builds in House to pass tax-cut package
4. House Democratic leader Steny Hoyer sees ‘very good things’ in the tax-cut deal, which many representatives oppose. But with the bill set to clear the Senate, reluctant House
5. Democrats are feeling the heat to pass it.

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 8 of 31

1. By Lisa Mascaro, Tribune Washington Bureau1
2. After the minor edits by ngarcia, the article’s title and byline allegedly read:
3. Pressure builds in House to elect CHIPPY 1337
4. House Democratic leader Steny Hoyer sees ‘very good things’ in the deal cut which will see uber skid Chippy 1337 take his rightful place, as head of the Senate, reluctant House
5. Democrats told to SUCK IT UP.
6. By CHIPPYS NO 1 FAN, Tribune Washington Bureau
7. The article’s substantive content was not altered, and website administrators restored the original in less
8. than an hour.

# I. THE SEARCH WARRANT AND AFFIDAVIT.

1. On October 3, 2012, Special Agent Gabriel Andrews (“Andrews”) submitted an “Application
2. and Affidavit for Search Warrant” to search Mr. Keys’ residence in Seacaucus, New Jersey. (Attached
3. hereto as Def.’s Ex. A.) United States Magistrate Judge Michael A. Hammer signed the warrant. The
4. warrant is in four parts: Attachments A, B, C, and D. Attachment A describes the place to be searched;
5. Attachment B describes the items to be seized; and Attachment C names the alleged offenses for which
6. the government sought evidence.
7. Attachment D of the search warrant is Andrews’ affidavit in support thereof. (See Def.’s Ex. A,
8. Attachment D (“Andrews Aff.”).) In October 2010, Mr. Keys was employed at KTXL Fox 40 (“Fox
9. 40”) in Sacramento as a “Web Producer.” (Andrews Aff. at ¶ 8.) Among other things, Mr. Keys’
10. responsibilities included managing Fox 40’s Facebook and Twitter accounts. (*Id.*) Near the end of that
11. month, a Fox 40 employee named Brandon Mercer—referred to in the affidavit only as the
12. “Producer”—allegedly terminated Mr. Keys’ employment. (*Id.*) According to Mercer, Mr. Keys then
13. changed the passwords to the Facebook and Twitter accounts, deleted 6,000 followers, and posted
14. headlines from other, competing stations. (*Id.*) After four days, Mercer regained control of the
15. accounts. (*Id.*) 25

26

27

1 The original article is still available on the Los Angeles Times website, at <http://articles.latimes.com/2010/dec/14/news/la->

28 pn-hoyer-tax-vote-20101215.

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 9 of 31

# A. EARLY DECEMBER 2010 “SUSPICIOUS” E-MAILS.

1. Next, Andrews’ affidavit describes some “suspicious” e-mails from a number of free e-mail
2. accounts: foxmulder4099@yahoo.co.uk, cybertroll69x@hotmail.com, walterskinner5099@yahoo.co.uk,
3. cancerman4099@yahoo.co.uk, and fox40truthers@gmail.com. (Andrews Aff. at ¶¶ 9-15.) These e-
4. mails were related to an alleged compromise of the “P2P Server,” a server owned by Tribune Media,
5. Fox 40’s parent company. (*Id.* at ¶ 7.)
6. On December 1, 2010, foxmulder4099@yahoo.co.uk allegedly sent Mercer a message
7. suggesting the writer had obtained e-mail addresses of all Fox 40 customers. (Andrews Aff. at ¶ 9.) The
8. two exchanged several emails, and foxmulder4099 continued to disparage Fox 40’s business practices. 10 (*Id.*)
9. The next day, cybertroll69x@hotmail.com sent Mercer an e-mail. (Andrews Aff. at ¶ 10.) This
10. e-mail contained a forwarded copy of a different e-mail message, allegedly sent from Fox 40 employee
11. “J.H.” (*Id.*) The message from J.H. claimed that foxmulder4099 was Mr. Keys. (*Id.*) When questioned
12. about the e-mail by Mercer, J.H. denied sending the message accusing foxmulder4099 of being Mr.
13. Keys. (*Id.*) According to Andrews’ affidavit, the person who created the cybertroll69x account claimed
14. to be Mr. Keys, and registered the account using a Sacramento zip code, 95824. (*Id.* at ¶ 11.) Andrews
15. identified IP address 98.208.49.74 as the only address used to access the account. (*Id.*) This address
16. “resolved to a location in Sacramento, California.” (*Id.*) Further attempts to identify cybertroll69x were
17. not successful. (*Id.*)
18. On December 3, Fox 40 received a strange e-mail from CancerMan4099@yahoo.co.ok.
19. (Andrews Aff. at ¶ 12.) Like the previous e-mail, CancerMan4099’s e-mail contained a forwarded copy
20. of a different message. (*Id.*) The forwarded message was from the American Cancer Society to
21. CancerMan4099, and it indicated that CancerMan4099 had given his contact name as “Matthew Keys”
22. to the American Cancer Society. (*Id.*) That same day a Fox 40 “customer” reported receiving an
23. unsolicited e-mail from fox40truthers@gmail.com. (*Id.* at ¶ 13.)
24. Finally, on December 6, 2010, Mercer received an e-mail in the form of a press release from
25. WalterSkinner5099@yahoo.co.uk. (Andrews Aff. at ¶ 14.) This e-mail referred to Mercer’s Facebook
26. page. (*Id.*)

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 10 of 31

* 1. Andrews’ affidavit explains why he included IP address information for only the
	2. cybertroll69x@hotmail.com account:
	3. “Fox Mulder,” “Walter Skinner,” and “Cancer Man” are characters from the Fox television show “The X-Files.” Subpoenas issued for these accounts determined either
	4. that the information was unavailable or that the account used was by a proxy server.

Based on my training and experience, I am aware that proxy servers are used by people

* 1. on the Internet to avoid having their activity traced back to them.
	2. (Andrews Aff. at ¶ 15.)
	3. Though Andrews’ affidavit made no mention of it, FBI agent John Cauthen expressed doubts
	4. about Mr. Keys’ involvement in the alleged breach of the P2P server. In a report dated Feb 14, 2011,
	5. Cauthen wrote a note: “Given the effort to hide the identity of the sender via the use of fake e-mails and
	6. proxy servers, it seems incongruous for the subject, if it is indeed Matthew Keys, to send out an e-mail
	7. identifying himself by name.” (*See* Feb. 11 Report of John Cauthen, attached hereto as Def.’s Ex. B.)
	8. The same report mentions that Mr. Keys was himself a victim of a compromised Twitter account. (*Id.*)
	9. Based in part on these facts, Cauthen wrote, “it appears Matthew Keys may not have been the subject
	10. behind the compromise at FOX40.” (*Id.*) Another report dated June 6, 2011 authored by Cauthen
	11. expressed similar sentiments. (*See* June 6 Report of John Cauthen, attached hereto as Def.’s Ex. C.) He
	12. thought it “illogical that the real hacker would identify himself so obviously while going to such lengths
	13. to avoid detection through the use of proxy servers.” (*Id.*) He thought Mr. Keys was “genuinely
	14. baffled” by allegations he compromised the e-mail server. (*Id.*) Rather, Cauthen viewed Mr. Keys’
	15. involvement as “likely only a journalistic interest. (*Id.*)

# B. COMMUNICATION BETWEEN MERCER AND MR. KEYS REGARDING

* 1. **ANONYMOUS.**
	2. On December 12, 2010, using Matthew@sactownmedia.com, Mr. Keys sent Mercer an e-mail.
	3. (Andrews Aff. at ¶ 16.) In the e-mail, Mr. Keys stated he “had infiltrated the group Anonymous,”2 and 24

25

26

2 Andrews’ affidavit does not elaborate on who or what the group Anonymous is. A proper treatment would require volumes,

1. but for the purposes of this Motion it suffices to describe Anonymous as an informal international collective of digital activists. They are known for the high-profile “hacktivist” (a portmanteau of hacker and activist) actions of some of the
2. members.

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 11 of 31

1 told Mercer he “had access to future Anonymous operations, including against the Los Angeles Times. 2 (*Id.*)

1. Around the same time, Mercer and Mr. Keys spoke by phone. (Andrews Aff. at ¶ 17.)
2. According to Mercer, Mr. Keys claimed he had access to a private chat room with “15 highly skilled
3. hackers” affiliated with Anonymous. (*Id.*) Mercer confronted Mr. Keys about the suspicious e-mails
4. discussed above, and Mr. Keys denied any involvement. (*Id.*)

# C. INTERNAL INVESTIGATION OF THE DECEMBER 14, 2010 EDITS TO THE

1. **LOS ANGELES TIMES WEBSITE.**
2. Andrews’ affidavit states that based on an internal investigation, the person who altered the Los
3. Angeles Times headline used Tribune CMS accounts “Anon1234” and “Arseface.” (Andrews Aff. at
4. ¶ 18.) And a Tribune employee observed a user named “sharpie” taking credit for the edits in some
5. “Anonymous IRC channels.” (*Id.*)

# D. MR. KEYS PUBLISHED ARTICLES ACKNOWLEDGING ACCESS TO “TOP

1. **LEVEL HACKERS” USING THE NAME “AESCracked.”**
2. In March and June 2011, Mr. Keys published articles on his website, producermatthew.com,
3. acknowledging that he had access to the private “internetfeds” chatroom, that he had provided the
4. Gawker website (gawker.com) with “one of dozens of logs” taken during that access, that he had
5. identified himself as a journalist, and that he had observed the notorious “Sabu” in the chatroom.
6. (Andrews Aff. at ¶¶ 19-20.) Mr. Keys also acknowledged providing screenshots to Parmy Olson, author
7. of *We Are Anonymous* [Little, Brown and Co, 2012]. (*Id.* at ¶¶ 27-28.)
8. On March 6, 2011, Mr. Keys published a screenshot of his participation in the chatroom.
9. (Andrews Aff. at ¶ 21.) Two images of this screenshot are attached as exhibits to Andrews’ affidavit.
10. (*See id.*) The screenshot shows Colloquy, a chat program, in a chatroom. (*Id.*) Although Mr. Keys’
11. username was mostly blurred, the screenshot appears to show that it ended with a “d” and that another
12. user referred to the username as “AES.” (*Id.*)

# E. CHAT LOGS SEIZED DURING OTHER INVESTIGATIONS.

1. In December 2011, investigators discovered a chat log seized pursuant to a search warrant in
2. which the username “Kayla” expresses a belief that Mr. Keys was AESCracked. (Andrews Aff. at ¶ 22.)

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 12 of 31

1. Kayla also wrote, “lol he’s not so innocent and we have logs of him too, he was the one who gave us
2. passwords for the LA times, fox40 and some others, he had superuser on a lot of media.”
3. Around the same time, Andrews discovered logs obtained during a different search of “digital
4. media” belonging to a person alleged to have used the name “Owen” and “Iowa.” (Andrews Aff. at
5. ¶ 23.) In these logs, AESCracked says, “i’m not a hacker. [¶] i’m an ex-employee . . . user: anon1234
6. [¶] pass: common2 [¶] go fuck some shit up!” (*Id.*) This username/password combination allegedly
7. granted access to the Tribune Company CMS. (*Id.* at ¶ 24.) Other logs from this seizure, attached to the
8. affidavit as Exhibit C, suggest that (a) AESCracked asked if anyone was interested in defacing the LA
9. Times; (b) AESCracked claimed to be an ex-employee; (c) AESCracked asked if anyone wanted to
10. purchase an e-mail list; and (4) AESCracked did all this in the “internetfeds” and “Operation Payback”
11. chatrooms. (*Id.*)

# F. OTHER IP ADDRESS INFORMATION.

1. Andrews’ affidavit states that at an unspecified date and time in January 2011 AESCracked used
2. IP address 78.129.220.46 to connect to a channel on the AnonOps chat server. (Andrews Aff. at ¶ 25.)
3. This address “was the one used by the sender of an e-mail from ‘foxmulder4099@yahoo.co.uk’ to Fox
4. 40 as described . . . above.” (*Id.*) On January 5, 2011, shortly after AESCracked was banned from the
5. same server, “A2SCracked” connected using IP address 75.53.171.204, which was allegedly registered
6. to Mr. Keys at the time. (*Id.* at ¶ 25.)

# G. JUSTIFICATION FOR THE BREADTH OF THE SEARCH.

1. Attachment B to the warrant application provides a boilerplate list of the items Andrews sought
2. to “search, copy, image and seize”:
3. a. Any computer equipment or digital devices belonging to MATTHEW KEYS that are
4. capable of being used to commit the Specified Federal Offenses, or to create, access,
5. or store evidence, or instrumentalities of such crimes, as set forth in Attachment B;
6. b. Any computer equipment or digital devices belonging to MATTHEW KEYS used to
7. facilitate the transmission, creation, display, encoding, or storage of data, including
8. word processing equipment, modems, docking stations, monitors, printers, plotters,
9. encryption devices, and optical scanners that belong to KEYS and are capable of

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 13 of 31

1. being used to commit or further the crimes outlined above, or to create, access,
2. process, or store evidence and instrumentalities of such crimes, as set forth in
3. Attachment B;
4. c. Any magnetic, electronic, or optical storage device capable of storing data, such as
5. floppy disks, hard disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks,
6. printer or memory buffers, smart cards, PC cards, memory calculators, electronic
7. dialers, electronic notebooks, personal digital assistants, and cell phones belonging to
8. MATTHEW KEYS that are capable of being used to commit or further the crimes
9. outlined above, or to create, access, or store evidence and instrumentalities of such
10. crimes, as set forth in Attachment B;
11. d. Any documentation, operating logs, and reference manuals regarding the operation of
12. the computer equipment, storage devices, or software belonging to MATTHEW
13. KEYS;
14. e. Any applications, utility programs, compilers, interpreters, and other software
15. belonging to MATTHEW KEYS used to facilitate direct or indirect communication
16. with the computer hardware, storage devices, or data belonging to KEYS to be
17. searched;
18. f. Any physical keys, encryption devices, dongles, or similar physical items belonging
19. to MATTHEW KEYS which are necessary to gain access to KEYS’s computer
20. equipment, storage devices, or data;
21. g. Any passwords, password files, test keys, encryption codes, or other information
22. belonging to MATTHEW KEYS necessary to access the computer equipment,
23. storage devices, or data; and
24. h. All records, documents, programs, applications, or materials created, modified, or
25. stored in any form, including digital form, on any computer or digital devices
26. belonging to MATTHEW KEYS, that show the actual user(s) of the computers or
27. digital devices during any time period in which the device was used to commit the
28. crimes referenced above, including the web browser’s history; temporary Internet

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 14 of 31

1. files; cookies, bookmarked, or favorite web pages; email addresses used from the
2. computer; MAC IDs and/or Internet Protocol addresses used by the computer; email,
3. instant messages, and other electronic communications; address books; contact lists;
4. records of social networking and online service usage; and software that would allow
5. others to control the digital device such as viruses, Trojan horses, and other forms of
6. malicious software (or alternatively, the lack of software that would allow others to
7. control the device).
8. i. All records, documents, programs, applications, or materials created, modified, or
9. stored in any form, including digital form, on any computer or digital device
10. belonging to MATTHEW KEYS, that show evidence of counter-forensic programs
11. (and associated data) that are designed to eliminate data from the computer or digital
12. device.
13. j. All records, documents, programs, applications, or materials created, modified, or
14. stored in any form, including in digital form, on any computer or digital device
15. belonging to MATTHEW KEYS, that show contextual information necessary to
16. understand the evidence, contraband, fruits, or instrumentalities described in
17. Attachment B.
18. (See Def.’s Ex. A, Attachment B.) Andrews offered the following boilerplate justification for this broad
19. seizure:
20. a. Searching computer systems is a highly technical process which requires specific
21. expertise and specialized equipment. There are so many types of computer hardware
22. and software in use today that it is impossible to bring to the search site all of the
23. necessary technical manuals and specialized equipment necessary to conduct a
24. thorough search. In addition it may also be necessary to consult with computer
25. personnel who have specific expertise in the type of computer, software application
26. or operating system that is being searched.
27. b. Searching computer systems requires the use of precise, scientific procedures which
28. are designed to maintain the integrity of the evidence and to recover “hidden,” erased,

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 15 of 31

1. compressed, encrypted or password-protected data. Computer hardware and storage
2. devices may contain “booby traps” that destroy or alter data if certain procedures are
3. not scrupulously followed. Since computer data is particularly vulnerable to
4. inadvertent or intentional modification or destruction, a controlled environment, such
5. as a law enforcement laboratory, is essential to conducting a complete and accurate
6. analysis of the equipment and storage devices from which the data will be extracted.
7. c. The volume of data stored on many computer systems and storage devices will
8. typically be so large that it will be highly impractical to search for data during the
9. execution of the physical search of the premises. A single megabyte of storage space
10. is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage
11. space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text.
12. Storage devices capable of storing 500 gigabytes (GB) of data are now commonplace
13. in desktop computers. Consequently, each non-networked, desktop computer found
14. during a search can easily contain the equivalent of 250 million pages of data, which,
15. if printed out, would result in a stack of paper over ten miles high. Further, a 500 GB
16. drive could contain as many as approximately 250 full run movies or 450,000 songs.
17. d. Computer users can attempt to conceal data within computer equipment and storage
18. devices through a number of methods, including the use of innocuous or misleading
19. filenames and extensions. For example, files with the extension “.jpg” often are
20. image files; however, a user can easily change the extension to “.txt.” to conceal the
21. image and make it appear that the file contains text. Computer users can also attempt
22. to conceal data by using encryption, which means that a password or device, such as a
23. “dongle” or “keycard,” is necessary to decrypt the data into readable form. In
24. addition, computer users can conceal data within another seemingly unrelated and
25. innocuous file in a process called “stenography.” For example, by using stenography
26. a computer user can conceal text in an image file which cannot be viewed when the
27. image file is opened. Therefore, a substantial amount of time is necessary to extract 28

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 16 of 31

* 1. and sort through the data that is concealed or encrypted to determine whether it is
	2. evidence, contraband, or instrumentalities of a crime.
	3. (Andrews Aff. at ¶ 37.) “In light of these concerns,” Andrews requested permission to “search, copy,
	4. image and seize the computer hardware (and associated peripherals) that are believed to contain some or
	5. all of the evidence described in this warrant, and to conduct an off-site search of the image . . . .” (*Id.* at 6 ¶ 38, 38d.)

# II. EXECUTION OF THE WARRANT.

1. On October 4, 2012, agents conducted the seizure authorized by the warrant at Mr. Keys’
2. residence. The agents seized one laptop computer and two external hard drives. They also took a
3. number of photographs and conducted a recorded interview of Mr. Keys.
4. At about 1:30 am the night before the execution of the search warrant, Mr. Keys ate a snack and
5. took two 50 mg doses of Trazodone, also known as Desyrel, an anti-depressant often prescribed to
6. induce sleep. (Decl. of Matthew Keys (“Keys Decl.”) at ¶¶ 3, 4; *see also* Decl. of Dr. Barry Cogen
7. (“Cogen Decl.”) at ¶ 4.) The common side effects of Trazodone include confusion, fatigue, and
8. nervousness. (Cogen Decl. at ¶ 7.) Mr. Keys fell asleep between 2:00 and 2:30 am. (Keys. Decl. at
9. ¶ 5.) Awoken before 6:00 from a “deep sleep” by federal agents, he was “drowsy, confused and
10. forgetful.” (*Id.* at ¶¶ 7, 9.) Agents encouraged and obtained written and oral statements from Mr. Keys,
11. despite the fact that Mr. Keys had expressed concerns about his state of mind. (*Id.* at ¶ 8.)

# ARGUMENT

1. **I. THE SEARCH WARRANT AUTHORIZED AN OVERBROAD GENERAL SEARCH OF**
2. **ALL OF MR. KEYS’ ELECTRONIC MEDIA.**
3. By permitting the seizure of every conceivable type of electronic media, the October 3, 2012
4. search warrant was unconstitutionally overbroad and the modern equivalent of a general warrant. “It is
5. familiar history that indiscriminate searches and seizures conducted under the authority of ‘general
6. warrants’ were the immediate evils that motivated the framing and adoption of the Fourth Amendment.”
7. *Payton v. New York*, 445 U.S. 573, 583 (1980); see also *Coolidge v. New Hampshire*, 402 U.S. 443, 467
8. (1971) (the “specific evil . . . abhorred by the colonists . . . is not that of intrusion *per se*, but of a
9. general, exploratory rummaging in a person’s belongings”). To prevent the abuse of such indiscriminate

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 17 of 31

1. rummaging, the Fourth Amendment requires each warrant to “particularly describ[e] the place to be
2. searched, and the persons or things to be seized.” U.S. Const. amend. IV. That is, search warrants must
3. be specific. *United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993). “Specificity has two aspects:
4. particularity and breadth.” *Id.* (quoting *In re Grand Jury Subpoenas Dated December 10, 1987*, 926
5. F.2d 847, 856-57 (9th Cir. 1991)). Not only must a warrant “clearly state what is sought,” but its scope
6. must also be “limited by the probable cause on which the warrant is based.” *Id.* (same).
7. The Fourth Amendment’s specificity requirements make computer searches especially difficult.
8. On one hand, computers are particularly vulnerable to general rummaging. A single computer, hard
9. disk, or USB drive may contain information about every aspect of a person’s life. Even cheap storage
10. media can store millions of pages of information, personal pictures, and intimate details of one’s life.
11. Moreover, the content of a computer file may not be obvious without opening the file itself. The
12. government’s inability to determine whether a file is concealed, compressed, erased, or booby-trapped
13. without examining it creates a “powerful incentive to seize more rather than less: . . . Let’s take
14. everything back to the lab, have a good look around and see what we might stumble on.” *United States*
15. *v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1170-71 (9th Cir. 2010) (en banc) (per curiam)
16. (“*CDT III*”). The very nature of computer searches raises the ominous specter of general warrants.
17. On the other hand, it may be difficult for an officer applying for a search warrant to be very
18. specific. How many computers or storage devices does the suspect possess? And which ones are likely
19. to contain evidence? Did the suspect use a laptop computer, a tablet, or a smartphone? Further, the
20. technical aspects of computer searches can be complicated. Sorting through gigabytes of information
21. takes time. Information may be encrypted or otherwise unreadable. In rare instances, some hardware or
22. software “may contain ‘booby traps’ that destroy or alter data if certain procedures are not scrupulously
23. followed.” As such, courts have recognized a “legitimate need to scoop up large quantities of data, and
24. sift through it carefully for concealed or disguised pieces of evidence . . . .” *CDT III*, 621 F.3d at 1176.
25. This need, however, does not yield to the Fourth Amendment. 26

27

28

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 18 of 31

# A. IN ORDER TO CONDUCT WHOLESALE SEIZURES OF ELECTRONIC

* 1. **MEDIA, THE GOVERNMENT MUST PRESENT A FACTUAL BASIS FOR**
	2. **DOING SO, IT MUST FOLLOW A SEGREGATION PROTOCOL FOR**
	3. **IDENTIFYING RELEVANT INFORMATION, AND IT MUST RETURN**
	4. **IRRELEVANT INFORMATION.**
	5. To prevent every warrant authorizing a computer search from functioning as a general warrant,
	6. the Ninth Circuit requires such warrants follow a number of rules: (1) the government must provide a
	7. factual justification for a broad search and seizure of the computer; (2) the search must be monitored by
	8. a neutral, detached magistrate; (3) the government must seal and hold documents pending judicial
	9. approval of a further search; (4) large-scale removal is only appropriate where on-site sorting is
	10. infeasible and no there is no practical alternative; (5) the government must promptly return documents
	11. outside the scope of the search.
	12. These rules have their roots in a case decided before computers were commonplace. In *United*
	13. *States v. Tamura*, 694 F.2d 591 (9th Cir. 1982), the FBI served a warrant on a business’ accounting
	14. department for specific records. When the business’ employees refused to help the agents locate the
	15. specific records the warrant authorized them to seize, the agents seized all of the records for the years in
	16. question. *Id.* at 594-95. Despite taking “large quantities” of documents not described in the warrant, the
	17. government argued the search was nevertheless reasonable because “the documents were intermingled
	18. and it was difficult to separate the described documents from the irrelevant ones.” *Id.* at 595. The court
	19. rejected this argument:
	20. It is true that all items in a set of files may be inspected during a search, provided that sufficiently specific guidelines for identifying the documents sought are provided in the
	21. search warrant and are followed by the officers conducting the search. However, the

wholesale *seizure* for later detailed examination of records not described in a warrant is

* 1. significantly more intrusive, and has been characterized as ‘the kind of investigatory dragnet that the fourth amendment was designed to prevent.’ We cannot sanction the
	2. procedure followed by the Government in this case.
	3. *Id.* (emphasis in original) (internal footnote and citations omitted).
	4. The *Tamura* court provided guidance for the “comparatively rare” times when information
	5. “cannot feasibly be sorted on site.” *Tamura*, 694 F.2d at 595-96. The government should seal and hold
	6. the documents pending judicial approval for a further search. *Id.* A magistrate should grant prior

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 19 of 31

1. approval for “large-scale removal of material . . . *only where on-site sorting is infeasible and no other*
2. *practical alternative exists.*” *Id.* at 969 (emphasis added). “The essential safeguard required is that
3. wholesale removal must be monitored by the judgment of a neutral, detached magistrate.” *Id.* (footnote
4. omitted). Although such wholesale seizures may be more convenient without judicial participation, they
5. are not reasonable. *Id.* Moreover, the government must return out-of-scope documents after
6. segregation: any “unnecessary delay” may result in an “unreasonable and therefore unconstitutional
7. manner of executing the warrant.” *Id.* at 597.
8. Nearly twenty-five years later, in *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006), the
9. Ninth Circuit revisited *Tamura* in the context of a broad seizure of “all computer media.”
10. Acknowledging “significant problems” inherent in computer searches, the court nevertheless refused to
11. give the government an “automatic blank check” for broad computer searches and seizures. *Id.* at 974-
12. 75. Rather, to justify a wholesale seizure of electronic media, “the government must still demonstrate to
13. the magistrate *factually* why such a broad search and seizure authority is reasonable in the case at hand.”
14. *Id.* at 975 (emphasis in original). The court recognized that in some cases, the government will have “no
15. basis” for believing they will actually encounter “the kind of technological problems that would make an
16. immediate onsite search and selective removal of relevant evidence impracticable.” *Id.* To give teeth to
17. this preference for onsite searches over wholesale seizure, *Hill* requires “some threshold showing before
18. the government may ‘seize the haystack to look for the needle.’” *Id.*
19. Most recently, in *CDT III*, 621 F.3d 1162, an en banc panel of the Ninth Circuit again applied
20. *Tamura*’s logic to computer searches. “The point of *Tamura* procedures is to maintain the privacy of
21. materials that are intermingled with seizable materials, and to avoid turning a limited search for
22. particular information into a general search . . . .” *Id.* at 1170. While the government has a “legitimate
23. need” for broad computer searches, that need “creates a serious risk that every warrant for electronic
24. information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.” *Id.*
25. at 1176. To balance the needs of law enforcement with the privacy “at the heart of the Fourth
26. Amendment,” the en banc panel’s per curiam opinion endorsed *Tamura* as a “workable framework.” *Id.*

27 at 1177.

28

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 20 of 31

* 1. Here, the government failed to follow the Ninth Circuit’s precedents in *Tamura*, *Hill*, and *CDT*
	2. *III*. The wholesale seizure of Mr. Keys’ electronic media was not monitored by a neutral, detached
	3. magistrate. Nor did the government take any precautionary measures to prevent a general search.
	4. Rather the government seized everything so they could rummage in Mr. Keys’ personal and professional
	5. life at their leisure. The agents did not return any irrelevant documents or data to Mr. Keys until counsel
	6. received discovery. These failures violated the protective measures required by *Tamura* and *CDT III*.
	7. Furthermore, Andrews’ boilerplate affidavit describes the difficulty of computer searches in
	8. general terms, rather than in specific factual terms that apply to Mr. Keys case. It provides no basis to
	9. anticipate the need for any exotic forensic equipment or specialized personnel. Worse, Andrews can
	10. point to no reason to believe Mr. Keys’ data would be hidden or protected by sophisticated booby traps.
	11. Rather, the evidence in the affidavit suggests Mr. Keys was a run-of-the-mill Mac user without any
	12. special “hacking” skills. And while the data in modern storage media is often voluminous, and the
	13. content of a file may not be apparent until it is opened, neither of these facts explain why the FBI chose
	14. to seize everything, rather than simply copying the files. In short, the affidavit fails to provide a factual
	15. basis for wholesale seizure in this case, as *Hill* requires.

# B. THE WARRANT COMPLETELY IGNORES CHIEF JUDGE KOZINSKI’S

* 1. **GUIDELINES IN *COMPREHENSIVE DRUG TESTING III*.**
	2. Moreover, to assist government agents performing computer searches and seizures, Chief Judge
	3. Alex Kozinski’s five-judge concurrence in *Comprehensive Drug Testing III* provides five concrete
	4. guidelines, none of which were followed here. Chief Judge Kozinski’s guidelines are based largely on
	5. the reasoning in the court’s per curiam opinion. While not law,3 they are intended to provide the
	6. government “a safe harbor,” while at the same time protecting the values of the Fourth Amendment.
	7. *CDT III*, 621 F.3d at 1178 (Kozinski, C.J., concurring). In short form, these guidelines are: 24

25

1. 3 Chief Judge Kozinski’s guidelines were originally included in the panel’s majority opinion. *See United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1004-07 (9th Cir. 2009) (“*CDT II*”). However, the opinion was
2. subsequently revised, and the guidelines were moved to the plurality’s concurrence. *See CDT III*, 621 F.3d at 1183 (Callahan, J., concurring in part and dissenting in part) (“The concurrence is not joined by a majority of the en banc panel and
3. accordingly the suggested guidelines are not Ninth Circuit law.”).

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 21 of 31

* 1. 1. Magistrate judges should insist that the government waive reliance upon the plain
	2. view doctrine in digital evidence cases.
	3. 2. Segregation and redaction of electronic data must be done either by specialized
	4. personnel or an independent third party. If the segregation is to be done by
	5. government computer personnel, the government must agree in the warrant
	6. application that the computer personnel will not disclose to the investigators any
	7. information other than that which is the target of the warrant.
	8. 3. Warrants and subpoenas must disclose the actual risks of destruction of information
	9. as well as prior efforts to seize that information in other judicial fora.
	10. 4. The government's search protocol must be designed to uncover only the information
	11. for which it has probable cause, and only that information may be examined by the
	12. case agents.
	13. 5. The government must destroy or, if the recipient may lawfully possess it, return non-
	14. responsive data, keeping the issuing magistrate informed about when it has done so
	15. and what it has kept.
	16. *Id.* at 1180 (same) (internal citations omitted).
	17. The government ignored these guidelines. First, neither the government nor the authorizing
	18. magistrate made any mention of the plain view doctrine. Although Defendant does not expect the
	19. government to rely on the plain view doctrine in this case, the failure to acknowledge the slippery slope
	20. of electronic plain view demonstrates a disregard for the guidelines. Second, the government did not use
	21. “specialized personnel” or an “independent third party” to segregate relevant from irrelevant data.
	22. Instead, the government seized all of Mr. Keys’ media and removed it for leisurely rummaging. Third,
	23. the warrant provides no particular basis for the conjecture that there might be hidden, encrypted, or
	24. booby-trapped data. Andrews’ affidavit identified no “actual risks” of information destruction, and no
	25. *facts* supporting the proposition that Mr. Keys’ equipment or data may have been booby-trapped.
	26. Indeed, it fails to justify anything more intrusive than plugging in an external USB drive and
	27. copy/pasting data. Fourth, the warrant contains no particular search protocol. As a result, the
	28. government’s general search and seizure swept up large volumes of information without probable cause.

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 22 of 31

1. And fifth, the government has kept all information it seized. Although Mr. Keys has received a copy of
2. his own data, he was required to provide his own media. Nothing has been returned; indeed, the
3. indictment seeks forfeiture of all electronic media seized pursuant to the warrant, without regard for its
4. relevance.
5. In sum, the October 3, 2012 warrant in this case authorized seizure of every conceivable kind of
6. electronic media, with no particularized search protocols or other safeguards to segregate relevant from
7. irrelevant information. It authorized the modern equivalent of a general search. The warrant was
8. unconstitutionally overbroad, and its fruits must be suppressed.

# II. AT THE TIME ANDREWS APPLIED FOR THE WARRANT, THE FACTS

1. **SUPPORTING PROBABLE CAUSE TO BELIEVE MR. KEYS POSSESSED ANY**
2. **EVIDENCE WERE STALE.**
3. Aside from the overbreadth problem, the facts in Special Agent Andrews’ supporting affidavit
4. were simply too stale to support the proposition that the October 4, 2012 search would turn up any
5. evidence of wrongdoing. Under the staleness doctrine, an affidavit supporting a search warrant “must
6. be based on facts so closely related to the time of the issue of the warrant as to justify a finding of
7. probable cause *at that time*.” *United States v. Lacy*, 119 F.3d 742, 745 (9th Cir. 1997) (quoting [*Durham*](http://scholar.google.com/scholar_case?case=9489932947034523173&amp;q=omission&amp;hl=en&amp;as_sdt=4%2C60%2C72%2C73%2C78%2C79%2C80%2C86%2C88%2C93%2C114%2C129%2C134%2C135%2C141%2C142%2C143%2C149%2C151%2C156%2C258%2C259%2C260%2C261%2C310%2C311%2C321%2C322%2C323%2C324%2C373%2C374%2C383&amp;as_ylo=2009)
8. [*v. United States*, 403 F.2d 190, 193 (9th Cir. 1968)](http://scholar.google.com/scholar_case?case=9489932947034523173&amp;q=omission&amp;hl=en&amp;as_sdt=4%2C60%2C72%2C73%2C78%2C79%2C80%2C86%2C88%2C93%2C114%2C129%2C134%2C135%2C141%2C142%2C143%2C149%2C151%2C156%2C258%2C259%2C260%2C261%2C310%2C311%2C321%2C322%2C323%2C324%2C373%2C374%2C383&amp;as_ylo=2009); [*Sgro v. United States*, 287 U.S. 206, 210, 53 S.Ct.](http://scholar.google.com/scholar_case?case=17637570021889456427&amp;q=omission&amp;hl=en&amp;as_sdt=4%2C60%2C72%2C73%2C78%2C79%2C80%2C86%2C88%2C93%2C114%2C129%2C134%2C135%2C141%2C142%2C143%2C149%2C151%2C156%2C258%2C259%2C260%2C261%2C310%2C311%2C321%2C322%2C323%2C324%2C373%2C374%2C383&amp;as_ylo=2009)
9. [138, 140 (1932)](http://scholar.google.com/scholar_case?case=17637570021889456427&amp;q=omission&amp;hl=en&amp;as_sdt=4%2C60%2C72%2C73%2C78%2C79%2C80%2C86%2C88%2C93%2C114%2C129%2C134%2C135%2C141%2C142%2C143%2C149%2C151%2C156%2C258%2C259%2C260%2C261%2C310%2C311%2C321%2C322%2C323%2C324%2C373%2C374%2C383&amp;as_ylo=2009)) (emphasis added) (internal quotation marks omitted). Staleness is evaluated “in light
10. of the particular facts of the case and the nature of the criminal activity and property sought.” *United*
11. *States v. Greany*, 929 F.2d 523, 525 (9th Cir. 1991). Thus, while a “significant gap in time can diminish
12. the probability that the evidence will be uncovered in the search,” see *United States v. Grant*, 682 F.3d
13. 827, 835 (9th Cir. 2012), the “mere lapse of substantial amounts of time is not controlling in a question
14. of staleness.” *United States v. Dozier*, 844 F.2d 701, 707 (9th Cir. 1988). Instead, the warrant should be
15. upheld if there is a “sufficient basis to believe, based on a continuing pattern or other good reasons, that
16. the items to be seized are still on the premises.” *United States v. Gann*, 732 F.2d 714, 722 (9th Cir.
17. 1984). Where “the evidence sought is of an ongoing criminal business of a necessarily long-term nature,
18. . . . rather than that of a completed act, greater lapses of time are permitted . . . .” *Greany*, 929 F.2d at 28 525.

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 23 of 31

* 1. Andrews’ affidavit provides no reason to suspect any “ongoing criminal business” justifying the
	2. lapse of time between the date of the crime, December 14, 2010, and the date of the warrant, October 3,
	3. 2012. The nearly 22-month delay is too long to support the search. *See United States v. Greathouse*,
	4. 297 F.Supp.2d 1264, 1272 (D. Or. 2003) (finding a thirteen month delay in Internet child pornography
	5. cases “simply too long . . . absent evidence of ongoing or continuous criminal activity”). Although at
	6. least one court has upheld a search for child pornography after a ten-month delay, that search was
	7. upheld because the affidavit in support of the warrants “provided ‘good reason’ to believe” the evidence
	8. would still be present. *See Lacy*, 119 F.3d 742, 746.
	9. Here, Andrews’ speculative justifications for the delay fall short of establishing probable cause
	10. that Mr. Keys retained evidence. He stated his belief that Mr. Keys would retain such evidence for so
	11. long because:
	12. (1) . . . there is probable cause to believe that KEYS participated in committing the Specified
	13. Federal Offenses;
	14. (2) evidence of Specified Federal Offenses, including the chat logs discussed in paragraph 21
	15. (*see also* Exhibits A and B attached hereto) was retained on KEYS’s computer as recently as

16 March 6, 2012, post-dating his move from Sacramento, California to Seacaucus, New Jersey;

1. (3) KEYS presently maintains the website [www.producermatthew.com,](http://www.producermatthew.com/) on which he has stated
2. that he actively monitors the Internet and updates his website from his residence;
3. (4) based on my training and experience, and the investigation to date, I know that KEYS is
4. proficient with computers and related technology, and that individuals such as KEYS
5. generally retain their computers and attendant digital media when moving from one residence
6. to another; and
7. (5) based on my training and experience, I am aware that data, even if deleted, will remain on a
8. computer until overwritten.
9. Andrews further stated his belief that Mr. Keys would retain data from his interaction with Anonymous
10. at home because “he regards this as an accomplishment that he wants to publish and receive credit for in
11. the future.” 28

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 24 of 31

* 1. These justifications fail for at least three reasons. First, and most obviously, there is “simply no
	2. evidence presented here of any ongoing criminal activity.” *Greathouse*, 297 F.Supp.2d at 1272.
	3. Probable cause that Mr. Keys participated in the LA Times edit is not itself probable cause that Mr.
	4. Keys would have evidence of it 22 months later, after a cross-country move. Second, the screenshot Mr.
	5. Keys posted to his website on March 6, 2012 was a screenshot, not “chat logs.” There is no evidence
	6. Mr. Keys ever recorded or kept any such chat logs. And just because a single file is published on a
	7. website does not mean that similar files reside on personal computing equipment, even where the
	8. administrator updates the site remotely from home. Third, and most troubling, Andrews’ affidavit relies
	9. on crude stereotypes of computer users and journalists. According to Andrews, “individuals such as
	10. KEYS”—those allegedly “proficient with computers and related technology”—are more likely to retain
	11. storage media for long periods of time. Similarly, because Mr. Keys was acting as a journalist during
	12. his interactions with Anonymous, Andrews’ hypothesized that he held on to his data to “receive credit
	13. for it in the future.” These generalizations lack foundation. The government cannot neuter the staleness
	14. doctrine for all journalists and other computer-proficient people on such a flimsy basis, without regard
	15. for the facts of the case.
	16. In short, by October 3, 2012, government agents no longer had probable cause to suspect that
	17. Mr. Keys possessed any evidence of the crime. Andrews failed to demonstrate any evidence of ongoing
	18. criminal activity, and his assertions that agents would find evidence of prior criminal activity were based
	19. on sleight-of-hand and crude generalizations. Under these circumstances, the warrant should be quashed
	20. and all evidence obtained therefrom suppressed.

# III. THE AFFIDAVIT CONTAINS DELIBERATE OR RECKLESS

* 1. **MISREPRESENTATIONS AND OMISSIONS REQUIRING A *FRANKS* HEARING.**
	2. It is well-settled that a defendant may challenge a warrant by challenging the truthfulness of
	3. statements therein. Where a defendant (1) “makes a substantial preliminary showing that a false
	4. statement knowingly and intentionally, or with reckless disregard of the truth, was included by the
	5. affiant in the warrant affidavit,” and (2) demonstrates that “the allegedly false statement is necessary to
	6. the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant’s
	7. request.” *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978) (“*Franks*”). To obtain a *Franks* hearing,

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 25 of 31

1. the defendant need not demonstrate “clear proof” of deception; the question of proof is “reserved for the
2. evidentiary hearing.” *United States v. Stanert*, 762 F.2d 775, 781 (9th Cir. 1985) (citing *United States v.*
3. *Chesher*, 678 F.2d 1353, 1362 (9th Cir. 1982)). *Franks* hearings are not limited to showings of false
4. affirmative statements, but are also appropriate where a warrant affidavit contains “deliberate or reckless
5. omissions of facts that tend to mislead.” *Stanert*, 762 F.2d at 780-81; *see also United States v. Jawara*,
6. 474 F.3d 565, 582 (9th Cir. 2007) (affirming *Stanert*). Where a warrant is challenged for omissions
7. tending to mislead, probable cause must be reconsidered with the omitted information included. *United*

8 *States v. DeLeon*, 979 F.2d 761, 764 (9th Cir. 1992).

# 9 A. ANDREWS’ AFFIDAVIT CONTAINS DELIBERATE OR RECKLESSLY-MADE

1. **STATEMENTS AND OMISSIONS.**
2. The search warrant affidavit contains two misleading material omissions. First, Andrews
3. omitted any reference to FBI agent John Cauthen’s documented belief that Mr. Keys was not responsible
4. for the “suspicious e-mails” sent to Fox 40 in early December, 2010. Cauthen’s reports provide
5. compelling reasons to believe Mr. Keys was not responsible. It would have been “incongruous” and
6. “illogical” for Mr. Keys to disclose his identity in the suspicious e-mails. Indeed, Mr. Keys was
7. “genuinely baffled” by the idea. Cauthen’s opinion was that Mr. Keys’ interest in the hacking
8. community was “journalistic,” not criminal. Yet none of this information was disclosed in Andrews’
9. affidavit.
10. Second, Andrews’ selective use of IP address information overstates the precision of that
11. evidence. First, in discussing the “suspicious e-mails,” despite investigating each of them, Andrews
12. identified only a single IP address which he claims “resolved to a location in Sacramento, California.”4
13. Mr. Keys lived in Sacramento at the time and used AT&T as an Internet Service Provider. Yet
14. documents received in discovery indicate that this IP address was administered by Comcast. (*See*
15. Comcast Response to Government Subpoena, Def.’s Ex. D.) Andrews’ inclusion of this IP address and
16. its alleged location were calculated to implicate Mr. Keys, despite other evidence that did not point to 26

27

4 Andrews explained that “[s]ubpoenas for these [other] accounts determined either that the information was unavailable or

28 that the account used was by a proxy server.” (Andrews Aff. at ¶ 15.) He offered no further details.

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 26 of 31

1. him at all. Second, the only IP address Andrews tied to the “AESCracked” nickname was
2. 78.129.220.46, which fortuitously was allegedly also used by foxmulder4099@yahoo.co.uk.
3. Presumably, this is the IP address of a proxy server, which “acts as an intermediary for requests from
4. clients seeking resources from other servers.” (Andrews Aff. at ¶ 4f.) But neither Andrews’ description
5. of a proxy server nor his discussion of this IP address includes the fact that proxy servers often serve as
6. proxies for many people at a time. Nor does Andrews make any effort to explain the month-long gap in
7. time between foxmulder4099’s use of the IP address and AESCracked’s use of the IP address, or how
8. that time lapse affects the analysis. In short, Andrews’ use of IP address information was calculated to
9. highlight information pointing to Mr. Keys while minimizing information suggesting someone else was
10. responsible.
11. These omissions were not merely negligent. Andrews knew or should have known of Cauthen’s
12. opinions of the case. And his use of IP address information supports a finding of reckless or intentional
13. omission “because the false statements and omissions contained in the affidavit all *bolster* the case for
14. probable cause, which suggests the mistakes were not the product of mere negligence.” *Chism v.*
15. *Washington State*, 661 F.3d 380, 388 (9th Cir. 2011). As one district court recently acknowledged,
16. “[m]uch, if not all, of the cyber-evidence (the E-mail addresses and IP addresses used) will lead you to
17. an innocent person.” *Id.* at 391 (quoting Washington State Police training materials with approval).
18. Andrews singled out such “cyber-evidence” when it implicated Mr. Keys, but ignored it when it did not.
19. *Cf. id.* at 388 (finding it “conspicuous that . . . the omissions purged the affidavit of any reference to the
20. possibility that someone other than [the defendant] was responsible for the offending [computer-related
21. crimes]”). These omissions satisfy *Franks*’ first prong.

# B. WITH THE FALSE STATEMENTS AND OMISSIONS CORRECTED, THE

1. **AFFIDAVIT DOES NOT SUPPORT A FINDING OF PROBABLE CAUSE.**
2. With Cauthen’s opinions and a complete picture of IP addresses included, a reasonable
3. magistrate would be unlikely to find probable cause. A straightforward affidavit would included
4. Cauthen’s prior belief that Mr. Keys neither compromised the P2P server nor sent any of the “suspicious
5. e-mails.” This fatally undermines the probative value of those e-mails.

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 27 of 31

* 1. What is left of the affidavit? (1) Mr. Keys’ acknowledgements that, working as a journalist, he
	2. had “infiltrated” a private Anonymous chatroom; and (2) excerpts of chat logs allegedly seized from
	3. other systems which allegedly belonged to some other people who were also allegedly in the same
	4. chatroom during the some of the same times as “AESCracked.” Obviously, Mr. Keys’
	5. acknowledgement that he had infiltrated Anonymous as a journalist does not itself implicate him in any
	6. criminal activity; it is merely an admission of journalism. Journalism is not a crime. The chat logs,
	7. seized pursuant to other investigations with no clear connection to this case or to Mr. Keys, are
	8. unaccompanied by any facts supporting their authenticity or reliability. Even combined with Mr. Keys’
	9. admissions that he had participated in some chats, the logs do not support probable cause to believe that
	10. Mr. Keys was indeed responsible for any crimes.
	11. In sum, Mr. Keys has made a “substantial preliminary showing” that Andrews’ affidavit contains
	12. deliberate or recklessly-made material omissions. With the omissions corrected, the affidavit does not
	13. provide probable cause to suspect Mr. Keys of any criminal activity. Therefore, he is entitled to a
	14. *Franks* hearing.

# IV. THE FRUIT OF THE POISONOUS TREE DOCTRINE REQUIRES SUPPRESSION OF

* 1. **WRITTEN AND RECORDED STATEMENTS OF MR. KEYS.**
	2. It is well-established that statements obtained as a result of an unlawful search or seizure must be
	3. suppressed. Such statements have been dubbed “fruit of the poisonous tree.” *Nardone v. United States*,
	4. 308 U.S. 338, 341 (1939); *Wong Sun v. United States*, 371 U.S. 471 (1963). Unless the government can
	5. “purge the primary taint” by showing it would have inevitably obtained the statements from an
	6. independent source, the statements are inadmissible. *Brown v. Illinois*, 422 U.S. 590, 600 (1975); *see*
	7. *also Nix v. Williams*, 467 U.S. 431, 443 (1984) (“The independent source doctrine allows admission of
	8. evidence that has been discovered by means wholly independent of any constitutional violation.”).
	9. In this case, the police interview was a direct result of the search and seizure. There is no reason
	10. to believe the government could have obtained statements from Mr. Keys without first obtaining and
	11. executing its unlawfully overbroad general warrant. Mr. Keys’ statements are fruit of the poisonous tree
	12. and must be suppressed.

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 28 of 31

# V. MR. KEYS’ *MIRANDA* WAIVER WAS INVALID BECAUSE IT WAS NOT

1. **VOLUNTARY, KNOWING AND INTELLIGENT.**
2. Independently, the written and recorded statements obtained during the execution of the October
3. 3, 2012 search warrant must be suppressed because they were taken in violation of *Miranda v. Arizona*,
4. 384 U.S. 436, 86 S.Ct. 1602 (1966). A defendant in a criminal case is deprived of due process of law if
5. his conviction is founded, in whole or in part, upon an involuntary confession. *See Jackson v. Denno*,
6. 378 U.S. 368, 376 (1964). A defendant who objects to the admission of a confession on the ground that
7. it was involuntary has a constitutional right to an evidentiary hearing to determine the voluntariness of
8. the confession before it is heard by a jury. *Id*. at 376-77.
9. Before the government may introduce a defendant’s custodial, incriminating statements, it must
10. prove that the defendant voluntarily, knowingly, and intelligently waived his rights. *See Miranda*, 384 12 U.S. at 475; *Colorado v. Spring*, 479 U.S. 564, 573, 107 S.Ct. 851 (1987); *Derrick v. Peterson*, 924 F.2d
11. 813, 820 (9th Cir. 1990) (noting that a court must also find that the defendant understood his rights).
12. When a defendant challenges a *Miranda* waiver, the government must prove such waiver by a
13. preponderance of the evidence. *Colorado v. Connelly*, 479 U.S. 157, 168, 107 S.Ct. 515 (1986).

# A. MR. KEYS INVOLUNTARILY WAIVED HIS *MIRANDA* RIGHTS.

1. A statement is involuntary if it is “extracted by any sort of threats or violence [or] obtained by
2. any direct or implied promises, however slight, [or] by the exertion of any improper influence.” *United*
3. *States v. Guerrero*, 847 F.2d 1363, 1366 (9th Cir. 1988) (citation and internal quotation omitted). “A
4. confession is not voluntary if it is made by a person whose mental condition at the time was such that
5. the confession most probably was not the product of any meaningful act of volition.” *United States v.*
6. *Smith*, 638 F.2d 131, 133 (9th Cir. 1981) (citation and internal quotation omitted). Courts have held that
7. incriminating statements made by an intoxicated defendant were involuntary and inadmissible. *See*
8. *Gladden v. Unsworth*, 396 F.2d 373, 380 (9th Cir. 1968).
9. In order to determine whether a statement is voluntary, the court must weigh “whether,
10. considering the totality of the circumstances, the government obtained the statement by physical or
11. psychological coercion or by improper inducement so that the suspect’s will was overborne.” *Derrick v.*
12. *Peterson*, 924 F.2d at 817 (citation and internal quotation omitted). Courts will also consider factors

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 29 of 31

1. such as the defendant’s age and education; the length of the detention; whether the defendant was
2. offered food; the accused’s physical and mental characteristics; the accused’s experience with the
3. criminal justice system; the location of the interrogation; the conduct of the police officers; and the type
4. and length of questioning. *See, e.g.*, *Taylor v. Maddox*, 366 F.3d 992, 1013-14 (9th Cir. 2004); *Lucero*
5. *v. Kerby*, 133 F.3d 1299, 1311 (10th Cir. 1998); s*ee also* 18 U.S.C. § 3501 (“The presence or absence of
6. any of the above-mentioned factors to be taken into consideration by the judge need not be conclusive
7. on the issue of voluntariness ”).
8. Here, Mr. Keys’ interrogation started shortly before 6:00 a.m., October 4, 2012. Earlier that
9. morning, Mr. Keys took 100 mg of Trazodone—double his prescribed dosage—in order to induce sleep.
10. Within a few hours of taking the Trazodone and falling asleep, he was suddenly awoken when
11. government agents entered his bedroom in his New Jersey apartment stating that they needed to ask him
12. some questions. The agents started to question Mr. Keys almost immediately upon waking him up from
13. his sleep. Two agents separated him while the rest searched the house and spoke to Mr. Keys’
14. roommates. During this time, Mr. Keys was still under the influence of a full dose of Trazodone.
15. (Cogen Decl. at ¶ 8.) As a result, Mr. Keys’ mental state was clouded.
16. Because of this compromised mental state, Mr. Keys’ *Miranda* waiver was involuntary and his
17. statements are otherwise inherently unreliable. (*See* Cogen Decl. at ¶¶ 9-10.) Therefore, this Court
18. should suppress his written confession and any inculpatory statements he made during the interrogation.

# B. MR. KEYS DID NOT KNOWINGLY AND INTELLIGENTLY WAIVE HIS

1. ***MIRANDA* RIGHTS.**
2. In addition to voluntariness, a defendant’s *Miranda* waiver must also be knowing and intelligent.
3. *See Derrick v. Peterson*, 924 F.3d at 820; *see also Gladden*, 396 F.2d at 376. The waiver must be made
4. “with a full awareness both of the nature of the right to be abandoned and consequences of the decision
5. to abandon it.” *Moran v. Burbine*, 475 U.S. 412, 421 (1986). Reviewing courts must look to the
6. “totality of the circumstances surrounding the interrogation” to answer these inquiries. *Id.*; *see also*
7. *Tague v. Louisiana*, 444 U.S. 469, 471 (1980) (per curiam) (government failed to show that petitioner
8. had waived his *Miranda* rights because the arresting officer could not remember the statements that he
9. read to the petitioner from a notice of *Miranda* rights, whether he asked the petitioner if he understood

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 30 of 31

1. the rights, or whether he conducted any tests to determine if the petitioner was literate or otherwise
2. capable of understanding his rights).
3. Factors commonly considered by courts in determining whether a valid *Miranda* waiver occurred
4. includes a suspect’s intelligence, age, and physical and mental condition, and the explicitness of the
5. suspect’s *Miranda* waiver. *See United States v. Montoya-Arrubla*, 749 F.2d 700 (11th Cir. 1985)
6. (intoxication considered as possible evidence of an invalid waiver); *Sample v. Eyman*, 469 F.2d 819, 821
7. (9th Cir. 1972) (man’s severe emotional distress following his wife’s death precluded a finding of a
8. knowing and intelligent waiver of *Miranda* rights). An otherwise voluntary confession may be
9. inadmissible if the accused lacks the mental capacity to make a knowing and intelligent waiver. *See*
10. *United States v. Frank*, 956 F.2d 872, 876 (9th Cir. 1991) (citing *Moran*, 475 U.S. at 421); *see also*
11. *United States v. Garibay*, 143 F.3d 534, 537-38 (9th Cir. 1998) (defendant with limited English skills
12. and low mental capacity did not validly waive his *Miranda* rights). Like voluntariness, whether a
13. suspect knowingly and intelligently waives his *Miranda* rights is viewed in light of the totality of the
14. circumstances surrounding the interrogation. *See Colorado v. Spring*, 479 U.S. at 573 (internal citations
15. and quotations omitted).
16. Here, Mr. Keys was suddenly woken from a deep sleep by government agents after he consumed
17. Trazodone, a powerful sleep-inducing drug. The agents told Mr. Keys they had a search warrant, and he
18. was questioned by FBI agents Cauthen and Andrews. (*See* Transcript of FBI Interview, attached hereto
19. as Def.’s Ex. E.) According to the transcript, Cauthen hastily read Mr. Keys his *Miranda* rights and
20. began questioning him. (*Id.* at 1-2.) While the three were getting situated, Cauthen informed Mr. Keys
21. he was not going to be arrested today, but Cauthen was going to read him his rights. (*Id.*) After
22. Cauthen finished, Mr. Keys interrupted the interrogation by saying, “Before we all start . . . .” (*Id.* at 2.)
23. Cauthen acknowledged to Mr. Keys that he appeared uneasy, and that he would answer all of his
24. questions. (*Id.*) But Mr. Keys was never allowed to finish his thought. Neither Cauthen nor Andrews
25. asked Mr. Keys if he understood his rights. Instead, Cauthen interrupted Mr. Keys while he attempted
26. to speak immediately after he was mirandized.
27. Mr. Keys was woken up out of a bed early in the morning, by multiple FBI agents mere hours
28. after taking a powerful sleeping pill. The FBI agents simultaneously read Mr. Keys his *Miranda* rights

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 31 of 31

1. while showing him a voluminous search warrant issued for his home. (*See* Def.’s Ex. E.) When he
2. interrupted the interrogation, he was cut off by Cauthen; the conversation continued on to introductions
3. and questioning. *Id*. In light of the totality of the circumstances surrounding Mr. Keys’ interrogation, it
4. is clear that he did not understand the nature of the rights abandoned or the consequences of abandoning
5. them. Thus, Mr. Keys did not knowingly and intelligently waive his *Miranda* rights.
6. For the reasons argued above, any *Miranda* waiver by Mr. Keys during the October 4, 2012
7. interrogation was not voluntary, knowing, and intelligent. Therefore, this court should suppress the
8. written and oral statements subsequently obtained.

# CONCLUSION

1. For the reasons argued above, this court should suppress all electronic evidence seized and
2. statements obtained as a result of the October 3, 2012 search warrant and execution thereof.
3. Dated: December 13, 2013 13

By:\_ */s/ Jay Leiderman*

1. Jason S. Leiderman
2. Eric J. Lindgren

LAW OFFICES OF JAY LEIDERMAN

16

1. By:\_ */s/ Tor Ekeland*
2. Tor Ekeland

TOR EKELAND, P.C.

19

20 Attorneys for Defendant

MATTHEW KEYS

21

22

23

24

25

26

27

28